

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 12/58	A1	(11) International Publication Number: WO 00/57605
		(43) International Publication Date: 28 September 2000 (28.09.00)

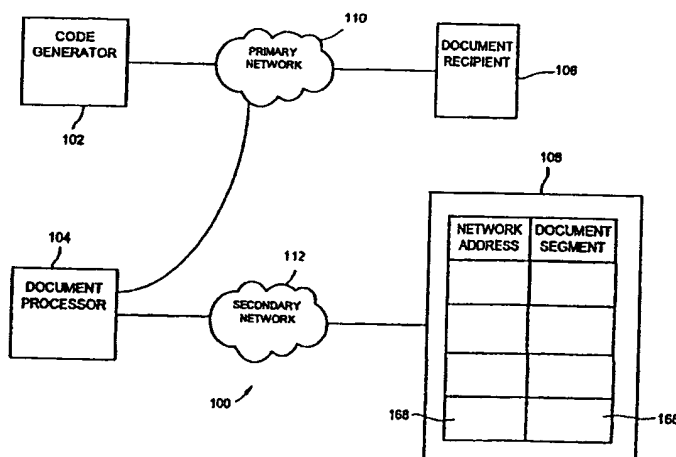
(21) International Application Number: PCT/CA00/00292
(22) International Filing Date: 22 March 2000 (22.03.00)
(30) Priority Data:
2,266,271 22 March 1999 (22.03.99) CA
(71) Applicant (for all designated States except US): RDM CORPORATION [CA/CA]; 608 Weber Street North, Unit #4, Waterloo, Ontario N2V 1K4 (CA).
(72) Inventor; and
(75) Inventor/Applicant (for US only): WALLACE, William, E. [CA/CA]; 97 William Street West, Waterloo, Ontario N2L 1J6 (CA).
(74) Agents: GRAHAM, Robert, J. et al.; Gowling Lafleur Henderson LLP, Suite 4900, Commerce Court West, Toronto, Ontario M5L 1J3 (CA).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DOCUMENT TRANSMISSION SYSTEM



(57) Abstract

A document transmission system is disclosed for transmission over a network of a document including at least one document segment. The document transmission system consists of a code generator, a document segment archive, and a document processor in communication with the document segment archive. The code generator is provided at one network location, and is configured to provide a document segment code which is uniquely associated with each document segment of the document. The document segment archive includes segment records associated with predefined document segments, with each document segment of the document having a corresponding predefined document segment in the document segment archive. Also, each segment record includes a code identifier uniquely associated with a respective one of the predefined document segments. The document processor is provided at a second network location. After the document is defined, the code generator transmits the segment codes associated with the document over the network to the document processor. The document processor then derives the document from the segment codes provided by the code generator.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KP	Democratic People's Republic of Korea	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KR	Republic of Korea	PL	Poland		
CM	Cameroon	KZ	Kazakhstan	PT	Portugal		
CN	China	LC	Saint Lucia	RO	Romania		
CU	Cuba	LJ	Liechtenstein	RU	Russian Federation		
CZ	Czech Republic	LK	Sri Lanka	SD	Sudan		
DE	Germany	LR	Liberia	SE	Sweden		
DK	Denmark			SG	Singapore		
EE	Estonia						

DOCUMENT TRANSMISSION SYSTEM

FIELD OF THE INVENTION

5 The present invention relates to a system for data transmission. In particular, the present invention relates to a method and system for the electronic transmission and reception of documents over a network.

10 BACKGROUND OF THE INVENTION

The widespread reach and appeal of the Internet and land-based enterprise networks is continually exposing network subscribers to an increasing volume and variety of information. As land-based network communication hardware technology, such as personal computers, servers and switching systems, has become more powerful, the
15 size and complexity of the documentation available to network subscribers has similarly increased.

At the same time, the advent of wireless communications devices, such as wireless telephones, pagers and personal data assistants, has greatly facilitated electronic
20 message communication between network subscribers. However, as the purpose of these devices has traditionally been to foster portable communications, wireless communications devices presently available are low in computing power and memory resources. Consequently, documentation of the size and complexity available to Internet and land-based enterprise network subscribers are not available to wireless
25 network subscribers.

Also, wireless communication is not a particularly secure form of message communication. With the appropriate wireless communication hardware, it is possible for unscrupulous individuals to intercept message information transmitted
30 over the wireless network, and to transmit message information to an intended recipient without the wireless recipient being aware that the transmitted information is erroneous.

-2-

Attempts have been made at rendering wireless message communication more secure. For instance, it is known to provide an encryption key for wireless telephones to ensure that the voice communications transmitted over the wireless network are not intercepted by third parties. However, this technology would not be suitable for document processing since the need for the wireless document reception device to encrypt and decrypt each wireless transmission would limit the ability of the device to transmit, receive, and display large complex documents.

Therefore, there remains a need for an electronic document transmission system which increases the size and complexity of the documentation available to wireless network subscribers. Further, there remains a need for an electronic document transmission system which facilitates secure document transmission over the wireless network.

15

SUMMARY OF THE INVENTION

According to the present invention, there is provided a document transmission system which addresses deficiencies of the prior art.

The document transmission system, according to the present invention, is provided for the transmission of a target document comprising at least one document segment. The document transmission system comprises a code generator, a document segment archive, and a document processor in communication with the document segment archive. The code generator is configured to provide a document segment code which is uniquely associated with each document segment of the document. The document segment archive includes segment records associated with predefined document segments, with each document segment of the document having a corresponding predefined document segment in the document segment archive. Also, each segment record includes a code identifier uniquely associated with a respective one of the predefined document segments. The document processor derives the target document from the segment codes provided from the code generator.

-3-

According to a second aspect of the present invention, there is provided a method for transmission of a target document over a network, comprising the steps of:

maintaining a document segment archive including segment records associated with predefined document segments, each said segment record including a code
5 identifier uniquely associated with a respective one of the predefined document segments;

at a first network location defining a document including at least one document segment, the at least one document segment corresponding to one of the predefined document segments;

10 providing at a second network location a segment code uniquely associated with the at least one document segment; and

at the second network location deriving the document from the segment code and a corresponding one of the segment records.

15 According to a third aspect of the present invention, there is provided a method for compressing a document which includes a plurality of document segments. The document compression method comprises the steps of:

providing a document segment archive comprising a plurality of predefined document segments;

20 providing a user interface for defining a document with reference to selected ones of the predefined document segments;

with the user interface choosing the selected predefined document segments;

providing segment codes uniquely associated with respective ones of the selected predefined document segments; and

25 retaining the segment codes in a storage medium, the selected predefined document segments associated with the retained segment codes when retained having conformity with the document.

30 According to a fourth aspect of the present invention, there is provided an electronic document which comprises a compressed document portion, an uncompressed document portion, and means for retaining the compressed document portion in fixed relation with the uncompressed document portion. The compressed document portion

-4-

includes at least one hash code uniquely, with each hash code being associated with a document segment disposed external to the compressed document portion. The uncompressed document portion includes text and/or graphics. The compressed document portion and the uncompressed document portion when so fixed are oriented
5 such that the uncompressed document portion and the document segment associated with the hash codes together define a coherent document.

According to a fifth aspect of the present invention, there is provided a message transmission system comprising a document processor, a document segment archive,
10 and a code generator in communication with the document processor and the document segment archive. The document processor is provided to define a message, for transmission, which includes at least one message segment. The document segment archive includes segment records associated with predefined document segments, with one of the predefined document segments corresponding to the at least
15 one message segment. Also, each segment record includes a code identifier uniquely associated with a respective one of the predefined document segments. The code generator provides the code identifier associated with the predefined document segment corresponding to the at least one document segment.

20 According to a sixth aspect of the present invention, there is provided a document storage system comprising a storage medium, a document archive and a plurality of electronic documents stored in the storage medium, and document selecting means for selecting one of the electronic documents. The document archive includes a plurality of document segments. Each electronic document comprises at least one data
25 structure, with each data structure including a segment code uniquely associated with one of the document segments. The document server also includes deriving means for deriving the selected electronic document in accordance with the respective data structures and the associated data document segments.

30

BRIEF DESCRIPTION OF THE DRAWINGS

-5-

The preferred embodiments of the invention will now be described, by way of example only, with reference to the drawings, in which:

Fig. 1 is a schematic diagram of a document transmission system, according to the present invention, showing the code generator for originating the document, the document segment archive, the document processor; and the document recipient;

Fig. 2 is a schematic diagram of the code generator depicted in Fig. 1, showing the code processor and the code transmitter;

Fig. 3 is a schematic diagram of the document processor and the document segment archive depicted in Fig. 1, showing the segment code receiver and the document server;

Fig. 4 is a schematic representation of a uncompressed document, and a document compressed according to the document transmission system;

Fig. 5 is a schematic diagram of a document transmission system, according to the present invention, for transmitting compressed messages directly between network users; and

Fig. 6 is a schematic diagram of a document storage system, according to the present invention, for storing the compressed documents depicted in Fig. 4.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Turning to Fig. 1, a document transmission system, denoted generally as 100, is shown comprising a code generator 102, a document processor 104, a document recipient 106, and a document segment archive 108. The document transmission system 100 also includes a primary network 110 interconnecting the code generator 102, the document processor 104, and the document recipient 106; and a secondary network 112 interconnecting the document processor 104 and the document segment

-6-

archive 108. Preferably, the primary network 110 comprises a wireless network, and the secondary network 112 comprises a land-based network, such as the Internet or enterprise network. However, the present invention is not limited to the network configurations shown in Fig. 1. For instance, the primary network 110 and the
5 secondary network 112 may be combined into a single network. Alternately, the document recipient 106 may communicate with the document processor 104 over the secondary network 112. Other network configurations will be apparent to those of ordinary skill in the art.

10 The code generator 102 is configured to provide document segment codes which are each uniquely associated with a desired document segment. Typically, the code generator 102 comprises a portable electronic communications device, such as a portable data assistant, or wireless telephone. As shown in Fig. 2, the code generator
15 102 comprises a user interface 114 for creating a desired document (comprising a plurality of document segments), a code processor 116 in communication with the user interface 114 for deriving segment codes for the document segments, and a document transmitter 118 in communication with the code processor 114 for
20 transmitting over the primary network 110 a compressed document which includes the segment codes. The user interface 114 comprises a data entry device 120, such as a keypad, a voice-recognition port, or a handwriting recognition device; and a display device 122 for viewing the desired document and the results of commands entered through the data entry device 120.

The code processor 116 comprises a central processing unit (CPU) 124, and a
25 programmable read-only memory (PROM) 126 and a read/write memory (RAM) 128 both in communication with the CPU 124. The PROM 126 includes processor instructions for the CPU 124. The processor instructions establish in the RAM 128 a memory object defining a document processor 130, a memory object defining a hash
code processor 132 in communication with the document processor 130, and a
30 memory object defining an encryption processor 134 in communication with the hash code processor 132. However, it will be appreciated that the document processor 130, the hash code processor 132, and the encryption processor 134 need not be

-7-

implemented as memory objects, but instead may be implemented in electronic hardware, if desired.

5 Preferably, the PROM 126 also includes a table 136 comprising a series of table entries, each comprising a hash code entry 138. Optionally, each table entry also specifies a network address entry 140 uniquely associated with each hash code entry 138. As will be discussed below, each hash code entry 138 is associated with a predefined document segment which is available over the secondary network 112, and each associated network address entry 140 is used by the document processor 104 to
10 construct the desired document.

The document processor 104 is configured to derive the desired document from the compressed document provided from the code generator 102. As shown in Fig. 3, the document processor 104 comprises a document receiver 142 for receiving compressed
15 documents from the code generator 102, a document server 144 in communication with the document receiver 142 for decompressing the received compressed documents, and a document transmitter 146 in communication with the document server 144 for transmitting the decompressed documents over the secondary network 112 to the intended document recipient 106. The document server 144 is also in
20 communication with the document segment archive 108 to assist in deriving the desired document from the compressed document.

The document server 144 comprises a central processing unit (CPU) 148 in communication with the document receiver 142, and a read-only memory (ROM) 150
25 and a R/W memory (RAM) 152 both in communication with the CPU 148. The ROM 150 includes processor instructions for the CPU 148. The processor instructions establish in the RAM 152 a memory object defining a decryption processor 154 for decrypting the received compressed documents, a memory object defining a hash code processor 156 in communication with the decryption processor 154 for verifying the
30 integrity of the compressed documents, and a memory object defining a document postprocessor 158 in communication with the hash code processor 156 for assembling the desired document from its corresponding document segment codes. Also, if the

PROM 126 does not include the table 136, described above, preferably the ROM 150 also includes a table 160 comprising a series of table entries, each comprising an unencrypted hash code entry 162 and a network address 164 uniquely associated with each unencrypted hash code entry 162. Alternately, the hash code entries 162 may
5 comprise public key encrypted hash code entries if all the transmitting users of the document transmission system are provided with the public encryption key.

The document segment archive 108 comprises an electronic database including a series of entries, each comprising a predefined document segment 166, and a network
10 address 168 associated with each predefined document segment 166. Preferably, the electronic database itself has a single network address within the secondary network 112. However, the predefined document segments may instead be spread over a plurality of electronic databases, with each database having its own network address within the secondary network 112. Further, preferably each predefined document
15 segment 166 comprises a text document segment, a graphics document segment, and audio document segment, or a document segment comprising a combination of text, graphics and/or audio.

Through the user interface 114 and the document segment processor 130, the user of
20 the code generator 102 creates a document 200 for transmission over the primary network 110, typically comprising a plurality of document segments, such as the graphic document segment 202 and the text document segments 204a, 204b, 206c shown schematically in the left half of Fig. 4. Preferably, the document segment processor 130 generates suitable document segment positional code for each
25 document segment 202, 204, such as with a Standard Generalized Markup Language (SGML)-based language, to define the relative orientation of the document segments 202, 204 within the document 200.

After the document 200 is defined, the document processor 130 transmits the
30 document segments 202, 204 to the hash code processor 132. The hash code processor 132 then derives a hash code for each of the document segments, with each hash code being uniquely associated with a respective one of the document segments.

-9-

However, it should be understood that the invention is not limited to the use of hash codes, and that other code formats may be utilized instead of hash codes.

5 If the PROM 126 includes the PROM table 136, the CPU 124 interrogates the hash code entries 138 with the hash codes generated from the hash code processor 132 to determine whether each associated document segment is available over the network 112. If a PROM table entry is located, and the PROM table 136 also includes network address entries 140, the CPU 124 retrieves the network address 140 associated with the hash code entry 138 which corresponds to the hash code from the hash code processor 132. The retrieved network address 140 comprises a document segment code which the CPU 124 preferably then joins with the corresponding document segment positional code data to form a compressed segment data structure. Alternately, if the PROM table 136 does not include any network address entries 140, the hash code entry from the PROM table 136 comprises the document segment code, 10 which the CPU 124 then preferably joins with the corresponding document segment positional code data to form the compressed segment data structure. 15

If no PROM table entry is located, the document segment is not available over the network 110, and the CPU 124 joins the document segment with the corresponding document segment positional code data to form a uncompressed segment data 20 structure. The compressed and uncompressed segment data structures comprise a compressed document which is ultimately transmitted over the primary network 110.

After each segment data structure is created, preferably the segment data structure is 25 then encrypted by the encryption processor 134. Preferably the encryption processor 134 encrypts each segment data structure with the private encryption key associated with the user of the code generator 102. As will be apparent, encryption with a private encryption key allows the recipient of the compressed document to verify that the transmitted document originated from the code generator user, if the recipient is 30 provided with the public encryption key corresponding to the private encryption key associated with the user of the code generator 102. However, it should be appreciated

-10-

that the encryption processor 134 is not an essential element of the invention, and may be eliminated if desired.

5 The resulting compressed document 200' is shown schematically in the right half of Fig. 4, which depicts the compressed document segment data structures 202', 204a', 204b', respectively corresponding to the document segments 202, 204a, 204b, and the uncompressed data structure 204c.

10 If the document transmission system 100 is configured such that the encryption processor 134 does not encrypt each segment data structure, preferably the hash code processor 132 hashes the segment data structures 202', 204' and any uncompressed document segments 202, 204. The encryption processor 134 then encrypts the resulting hash with the private key of the user of the code generator 102 so as to provide a digital signature 206 which the CPU 124 then appends to the compressed document 200'. As will be apparent, the digital signature 206 is used by the document processor 104 to ensure that the compressed document 200' was not altered during transmission over the primary network 110. However, it will be appreciated that provision of a digital signature 206 is not essential to the invention, and may be eliminated even if none of the segment codes are encrypted.

20 After the appended compressed document is completed, preferably the encryption processor 134 encrypts the appended compressed document with the public key of the document processor 104 so that the document can only be read by the document processor 104. The encrypted appended compressed document is then passed to the document transmitter 118 for transmission to the document processor 104 over the primary network 110.

25 After the encrypted appended compressed document is received by the document receiver 142, the decryption processor 154 decrypts the document with the private key of the document processor 104. If the compressed document 200' is appended with the digital signature 206, the decryption processor 154 then decrypts the digital signature 206 with the public key of the transmitting user. The decryption processor

154 may obtain the public key of the transmitting user through any suitable means, including via a digital certificate provided from a trusted certificate authority.

5 If the compressed document 200' is appended with the digital signature 206, the decryption processor 154 then passes the resulting compressed document 200' to the hash code processor 156 and the decrypted digital signature 206 to the document postprocessor 158. The hash code processor 156 derives the hash code for the compressed document 200', and passes the derived hash code to the document postprocessor 158. The document postprocessor 158 compares the hash code derived
10 by the hash code processor 156 with the hash code derived from the digital signature 206 to ensure that the compressed document 200' was not altered during transmission over the primary network 110. If the document postprocessor 158 is unable to verify the integrity of the compressed document 200', the document postprocessor 158 does not attempt to decompress the received document, as described below.

15 If the compressed document 200' does not have an appended digital signature 206, or if the document postprocessor 158 is able to verify the integrity of the compressed document 200', the document postprocessor 158 extracts the segment data structures 202', 204' from the compressed document 200'. If the extracted segment data
20 structures 202', 204' were encrypted with the transmitting user's private encryption key, the document postprocessor 158 passes each segment data structures 202', 204' to the decryption processor 154 for decryption. The document postprocessor 158 then extracts the segment codes from the compressed data structures 202', 204'.

25 If the document transmission system 100 is configured such that the segment data structures 202', 204' include the hash code of each compressed document segment, but do not specify the network address of each compressed document segment, the document postprocessor 158 then queries the hash code entries 162 of the table 160 of the ROM 150 with the hash codes from the segment data structures 202', 204' for the
30 network address 164 of each corresponding document segment. Alternately, the document postprocessor 158 obtains the network address 164 of each document

-12-

segment directly from the segment data structures 202', 204', if the segment data structures 202', 204' specify the network address of each document segment.

5 The document postprocessor 158 then queries the document segment archive 108 with the obtained network addresses to retrieve the desired document segments, and then assembles the desired document with the document segment positional code data for each document segment, including any uncompressed document segments. The assembled document is then transmitted via the document transmitter 146 to the document recipient 106 over the primary network 110.

10 Numerous applications of the foregoing embodiment are envisaged. For instance, in one application, the document transmission system 100 is used for electronic funds transfer, with the compressed document 200' comprising an electronic cheque. In this application, the bank of the payor (issuer) of the cheque comprises the document
15 processor 104. The payor generates a cheque with the code generator 102, specifying the name of the payee, the name of the payor's bank, the date, and the amount of funds to be paid. The user also includes as part of the cheque the user's bank account number, which becomes compressed and encrypted, as discussed above. Preferably, all of these items are encrypted with the payor's private encryption key to preclude
20 tampering. The user then transmits the compressed electronic cheque directly to the intended recipient 106 over the primary network 110, preferably after encrypting the cheque with the public encryption key of the intended recipient 106.

25 Upon receipt of the cheque, the recipient 106 decrypts the cheque with its private encryption key, and then electronically endorses the cheque. Preferably, the recipient 106 encrypts the endorsed cheque with the public encryption key of the recipient's bank, and then transmits the endorsed cheque to the recipient's bank. The recipient's bank then transmits the cheque to the payor's bank for settlement. Upon receipt of the endorsed cheque from the recipient's bank, the payor's bank queries its ROM table
30 160 with the compressed account number for an entry identifying the issuer's bank account number. The payor's bank then effects settlement of the cheque with the recipient's bank.

-13-

In another application, the invention is used for transmitting messages between portable electronic devices, preferably over a primary wireless network 110. In this application, each user is provided with the document transmission system 300, shown in Fig. 5. The document transmission system 300, is similar to the code generator 102 and the document processor 104, in that it comprises the user interface 114, the document transmitter 118, and the document receiver 142. However, in addition, the document transmission system 300 also includes a code segment processor 316 which comprises a central processing unit (CPU) 324, and a programmable read-only memory (PROM) 326 and a read/write memory (RAM) 328 both in communication with the CPU 324.

The PROM 326 includes processor instructions for the CPU 324. The processor instructions establish in the RAM 328 a memory object defining a document processor 330, a memory object defining an encryption processor 334, a memory object defining a decryption processor 354, a memory object defining a document postprocessor 358, and a memory object defining a hash code processor 332 in communication with the document processor 330, the encryption processor 334, the decryption processor 354, and the document postprocessor 358. It will be appreciated that any of the foregoing memory objects 330, 332, 334, 354, 358 may be implemented in electronic hardware instead, if desired. The PROM 326 also includes a table 336 comprising a series of table entries, each comprising a hash code entry 338, and a predefined document segment 366 uniquely associated with each hash code entry 338.

The operation of the document transmission system 300 is similar to the operation of the document transmission system 100. Through the user interface 314 and the document segment processor 330, the user creates a document 200 for transmission over the primary network 110, typically comprising a plurality of document segments 202, 204. The document processor 330 then transmits the document segments 202, 204 to the hash code processor 332 which derives a unique document segment code (hash code) for each document segments 202, 204.

-14-

The CPU 324 interrogates the hash code entries 338 in the PROM table 336 with the segment codes generated from the hash code processor 332 to determine whether each associated document segment is already defined. If a PROM table entry is located, the CPU 324 joins the segment code with the corresponding document segment
5 positional code data into a compressed segment data structure. If no PROM table entry is located, the CPU 324 joins the uncompressed document segment with the document segment positional code data into an uncompressed segment data structure. As discussed above, the compressed and uncompressed segment data structures 202', 204' comprise the compressed document 200'.

10

After each segment data structure 202, 204 is created, preferably the segment data structures are then individually encrypted by the encryption processor 334 with the private encryption key associated with the user of the document transmission system 300. Alternately, or additionally, the CPU 324 may append a digital signature 206
15 (created from the hash code processor 332 and the encryption processor 334) to the compressed document 200', as described above. As will be apparent, the encryption processor 334 is not an essential element of the invention, and may be eliminated if desired.

20 After the appended compressed document is completed, preferably the encryption processor 334 encrypts the appended compressed document with the public key of the target user so that the document can only be read by the target user. The encrypted appended compressed document is then retained in the RAM 328 until transmitted to the target user via the document transmitter 318.

25

The encrypted appended compressed document is received by the document receiver 142, and then decrypted by the decryption processor 354 with the private key of the target user. If the compressed document 200' is appended with the digital signature 206, the decryption processor 354 and the hash code processor 332 are used to verify
30 that the compressed document 200' was not altered during transmission over the primary network 110.

-15-

If the compressed document 200' does not have an appended digital signature 206, or if the document postprocessor 358 is able to verify the integrity of the compressed document 200', the document postprocessor 358 extracts the segment data structures 202', 204' from the compressed document 200'. If the extracted segment data
5 structures 202', 204' were encrypted with the transmitting user's private encryption key, the segment data structures 202', 204' are decrypted with the decryption processor 354. The document postprocessor 358 then extracts the segment codes from the compressed segment data structures 202', 204'.

10 The document postprocessor 358 then queries the hash code entries 338 of the table 336 of the PROM 326 with the segment codes extracted from the segment data structures 202', 204' for the desired document segments, and then assembles the desired document with the document segment positional code data for each document segment, together with any uncompressed document segments. The assembled
15 document is then transmitted to the user interface 114 of the recipient.

Another application of the invention is shown in Fig. 6. In Fig. 6, there is shown a document storage system 400 which is used for storing compressed documents and for retrieving and decompressing the compressed documents upon command.

20 Preferably the document storage system 400 is provided at a node within a network 310, with then network 310 including user terminals and peripheral devices. The document storage system 400 comprises the user interface 114, the document transmitter 118, a central processing unit (CPU) 424 in communication with the user interface 114 and the document transmitter 118, and a non-volatile storage 470 and a
25 read/write memory (RAM) 428 both in communication with the CPU 324.

Preferably, the non-volatile storage 470 comprises a magnetic disc storage device, and includes a document segment archive 408 and a compressed document archive 472 stored on the non-volatile storage 470. The document segment archive 408 comprises
30 a table including a series of table entries, each comprising a hash code entry 438, and a predefined document segment 466 uniquely associated with each hash code entry 438.

-16-

The compressed document archive 472 comprises a plurality of compressed electronic documents 200'. Typically, each compressed electronic document 200' comprises at least one compressed document segment data structure, and may also comprise an uncompressed data structure. Each compressed document segment data structure
5 includes positional code data, and a segment code uniquely associated with one of the predefined document segments 466.

The RAM 428 includes a memory object defining document selecting means 474 for selecting one of the compressed documents 200', and a memory object defining
10 deriving means 476 in communication with the document selecting means 474 for decompressing and deriving the selected document in accordance with the segment codes and positional code data defined in the compressed document 200' and in accordance with the data document segments associated with the segment codes.

15 In operation, a user selects a document from the document storage system 400 via the user interface 114 and the selecting means 474, and specifies the network address of the intended recipient user or peripheral device. The selecting means 474 retrieves the compressed document segment data structures and any uncompressed document segment data structures from the compressed document archive 472. The deriving
20 means 476 then decompresses the selected compressed document 200' by extracting the segment codes from the compressed document segment data structure, and then derives the selected document as described above. The document transmitter 118 then transmits the document to the intended recipient user or peripheral device.

25 The foregoing description is intended to be illustrative of the preferred embodiments of the present invention. Those of ordinary skill will envisage certain additions, deletions and/or modifications to the described embodiments which, although explicitly described herein, do not depart from the scope or spirit of the invention, as defined by the claims appended hereto.

-17-

I CLAIM:

1. A document transmission system for transmission of a document comprising at least one document segment, the document transmission system comprising:
 - a code generator for providing a document segment code, the segment code being uniquely associated with the at least one document segment;
 - a document segment archive including segment records associated with predefined document segments, one of the predefined document segments corresponding to the at least one document segment, each said segment record including a code identifier uniquely associated with a respective one of the predefined document segments; and
 - a document processor in communication with the document segment archive for deriving the document from the segment codes provided from the code generator.
2. The document transmission system according to claim 1, wherein the code generator comprises a code processor for deriving the segment code from the at least one document segment, and a transmitter coupled to the code processor for transmitting the derived segment code to the document processor.
3. The document transmission system according to claim 2, wherein the segment code comprises a hash code, and the code processor comprises a hash code processor for deriving the hash code from the at least one document segment.
4. The document transmission system according to claim 2, wherein the predefined document segments are available over a network, each said predefined document segment having a unique network address, and the code processor is configured for deriving the segment code from the network address associated with the predefined document segment corresponding to the at least one document segment.
5. The document transmission system according to claim 3 or 4, wherein the code processor includes an encryption processor for encrypting the segment code.

-18-

6. The document transmission system according to claim 5, wherein the encryption processor is configured for encrypting the derived hash code with a private encryption key.
7. The document transmission system according to any of claims 1 to 6, wherein the code generator includes a document generator for selecting the at least one document segment from a document segment set corresponding to the predefined document segments.
8. The document transmission system according to claim 2, wherein the transmitter comprises a wireless transmitter, and the document processor comprises a wireless receiver for receiving the transmitted segment code transmitted from the wireless transmitter, and a document server coupled to the wireless receiver and the document segment archive for identifying the predefined document segment associated with the received segment code.
9. The document transmission system according to claim 1, wherein the predefined document segments are available over a network, each said predefined document segment having a unique network address, and each said segment record includes a field identifying the network address associated with the respective predefined document segment.
10. The document transmission system according to claim 9, wherein each said code identifier comprises a hash code derived from the respective predefined document segment, and the document processor is configured for interrogating the hash code identifiers with the provided segment code.
11. The document transmission system according to claim 10, wherein each said hash code comprises an encrypted hash code.
12. A method for transmitting a document over a network, comprising the steps of:
maintaining a document segment archive including segment records associated with predefined document segments, each said segment record including a code identifier uniquely associated with a respective one of the predefined document segments;

-19-

at a first network location defining a document including at least one document segment, the at least one document segment corresponding to one of the predefined document segments;

providing at a second network location a segment code uniquely associated with the at least one document segment; and

at the second network location deriving the document from the segment code and a corresponding one of the segment records.

13. The method according to claim 12, wherein the providing step comprises the steps of deriving the segment code from the at least one document segments, and transmitting the derived segment code over the network from the first network location to the second network location.

14. The method according to claim 13, wherein the segment code comprises a hash code, and the segment code deriving step comprises deriving the hash code from the at least one document segment.

15. The method according to claim 13, wherein the predefined document segments are available over the network, each said predefined document segment having a unique network address, and the segment code deriving step comprises deriving the network address associated with the predefined document segment corresponding to the at least one document segment.

16. The method according to claim 14 or 15, wherein the segment code deriving step further comprises encrypting the derived segment code.

17. The method according to claim 16, wherein the encrypting step comprises encrypting the derived segment code with a private encryption key.

18. The method according to claim 12, wherein each said code identifier comprises a hash code derived from the respective predefined document segment, and the document deriving

-20-

step comprises the steps of interrogating the code identifiers with the provided segment code, and selecting a matching one of the predefined document segments.

19. The method according to claim 18, wherein each said hash code comprises an encrypted hash code.
20. A document delivered with the method according to any of claims 12 to 19.
21. The document according to claim 20, wherein the delivered document comprises a financial instrument.
22. A method for compressing a document, comprising the steps of:
 - providing a document segment archive comprising a plurality of predefined document segments;
 - providing a user interface for defining a document with reference to selected ones of the predefined document segments;
 - with the user interface choosing the selected predefined document segments;
 - providing segment codes uniquely associated with respective ones of the selected predefined document segments; and
 - retaining the segment codes in a storage medium, the selected predefined document segments associated with the retained segment codes when retained having conformity with the document.
23. The method according to claim 22, wherein the segment code providing step comprises deriving each said segment codes from the respective predefined document segment.
24. The method according to claim 23, wherein each said segment code comprises a hash code, and the segment code deriving step comprises deriving each said hash code from the respective predefined document segment.

-21-

25. The method according to claim 23, wherein the predefined document segments are available over a network, each said predefined document segment having a unique network address, and the segment code deriving step comprises deriving the network address associated with the respective predefined document segment.
26. The method according to claim 24 or 25, wherein each said segment code comprises an encrypted segment code, and the segment code deriving step further comprises encrypting each said derived segment code.
27. A document compressed with the method according to any of claims 22 to 26.
28. The document according to claim 27, wherein the compressed document comprises a compressed financial instrument.
29. An electronic document comprising:
a compressed document portion including at least one hash code uniquely associated with a document segment, the document segment being disposed external to the compressed document portion;
an uncompressed document portion including at least one of text and graphics; and
means for retaining the compressed document portion in fixed relation with the uncompressed document portion, the uncompressed document portion and the document segment associated with the at least one hash code so fixed together defining a coherent document.
30. The electronic document according to claim 29, wherein the document segment includes financial information.
31. The electronic document according to claim 29 or 30, further comprising a digital signature portion derived from the compressed and uncompressed document portions.
32. A message transmission system comprising:

-22-

a document processor for defining a message for transmission, the message comprising at least one message segment;

a document segment archive including segment records associated with predefined document segments, one of the predefined document segments corresponding to the at least one message segment, each said segment record including a code identifier uniquely associated with a respective one of the predefined document segments; and

a code generator in communication with the document processor and the document segment archive for providing the code identifier associated with the one predefined document segment corresponding to the at least one document segment.

33. A document storage system comprising:

a storage medium;

a document archive including a plurality of document segments;

a plurality of electronic documents each comprising at least one data structure, each said data structure including a segment code uniquely associated with one of the document segments, the document segments and the electronic documents stored together on the storage medium;

document selecting means for selecting one of the electronic documents; and

deriving means in communication with the document selecting means for deriving the selected electronic document in accordance with the respective data structures and the associated data document segments.

1/6

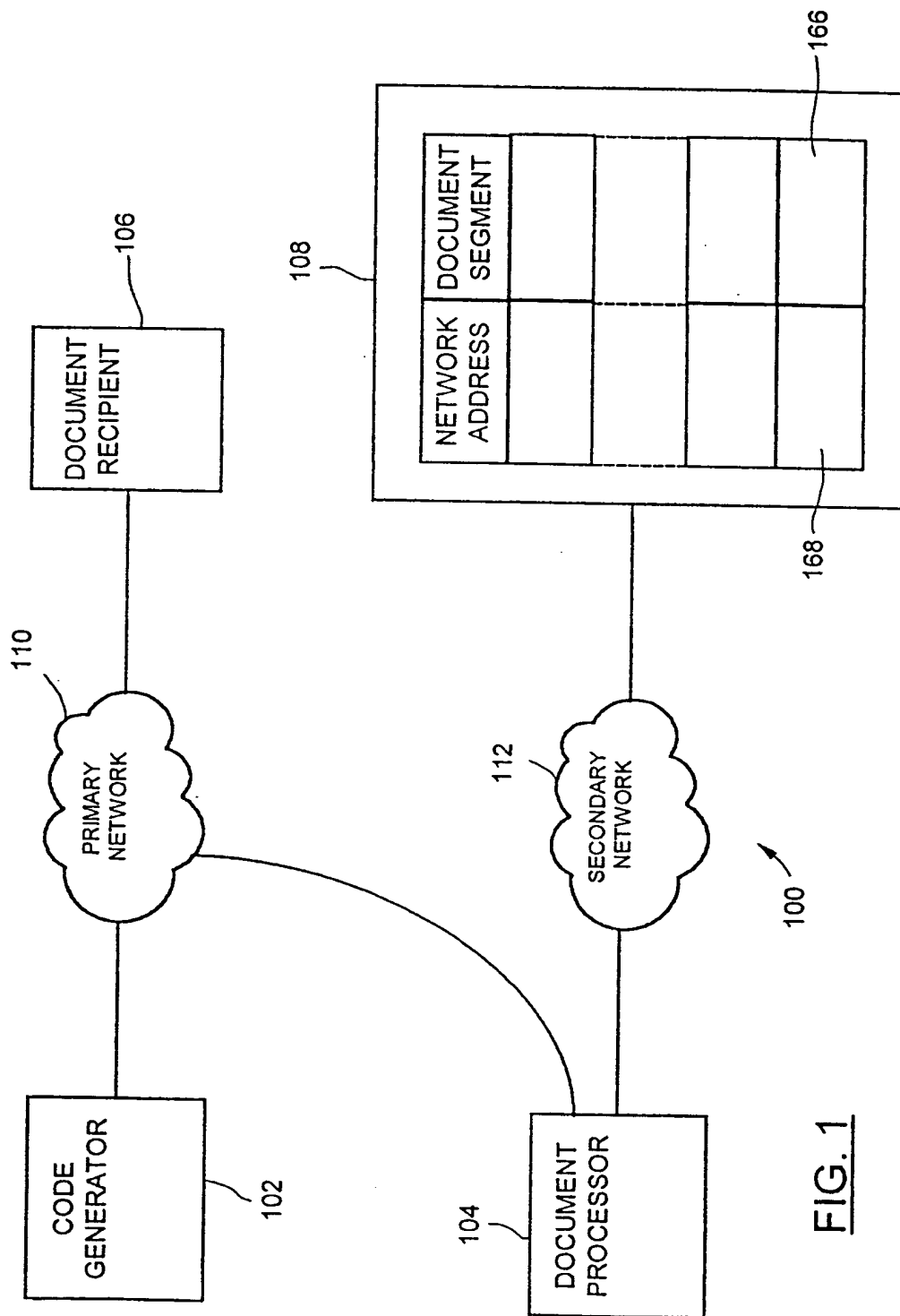


FIG. 1

2/6

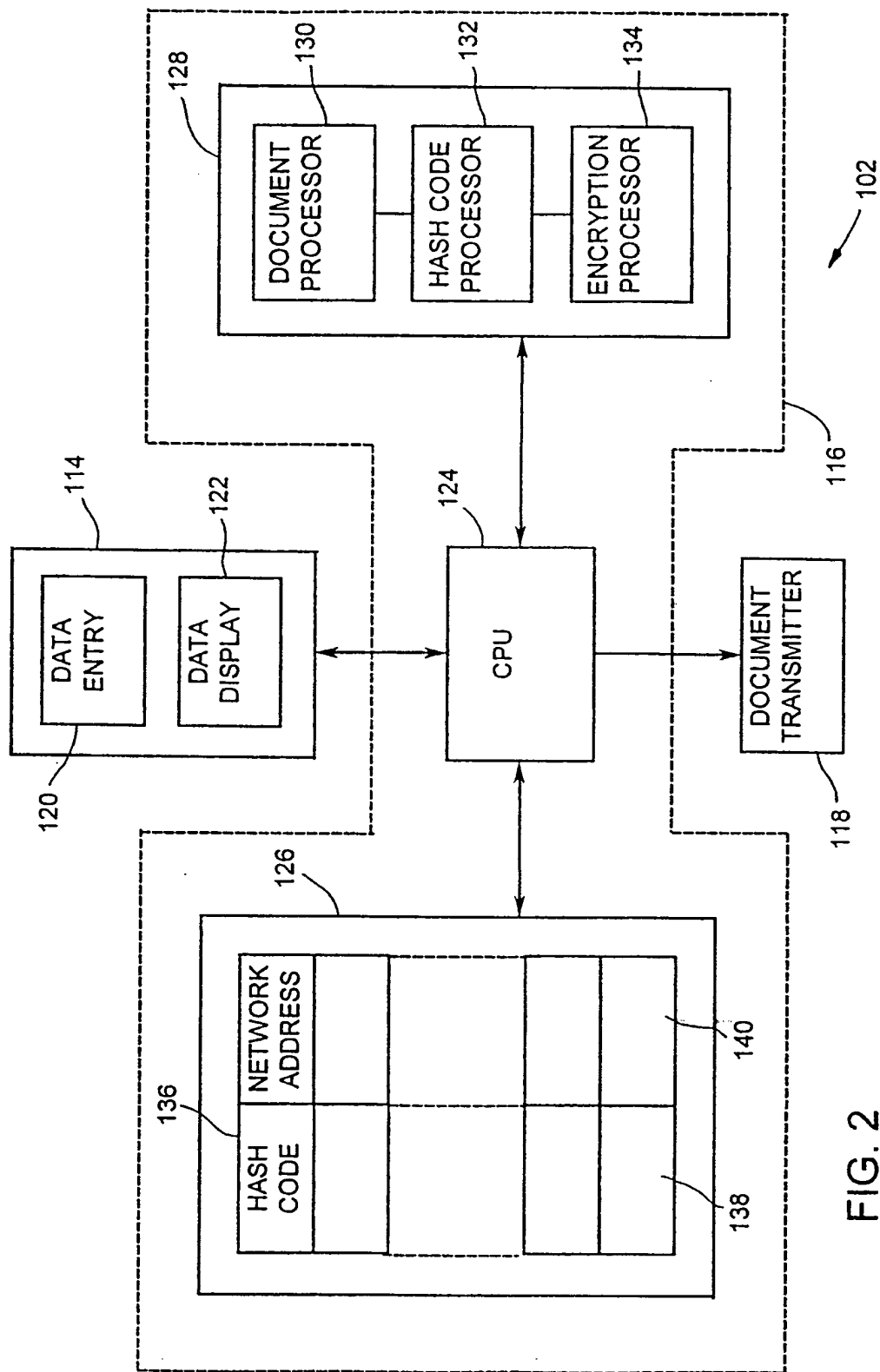


FIG. 2

3/6

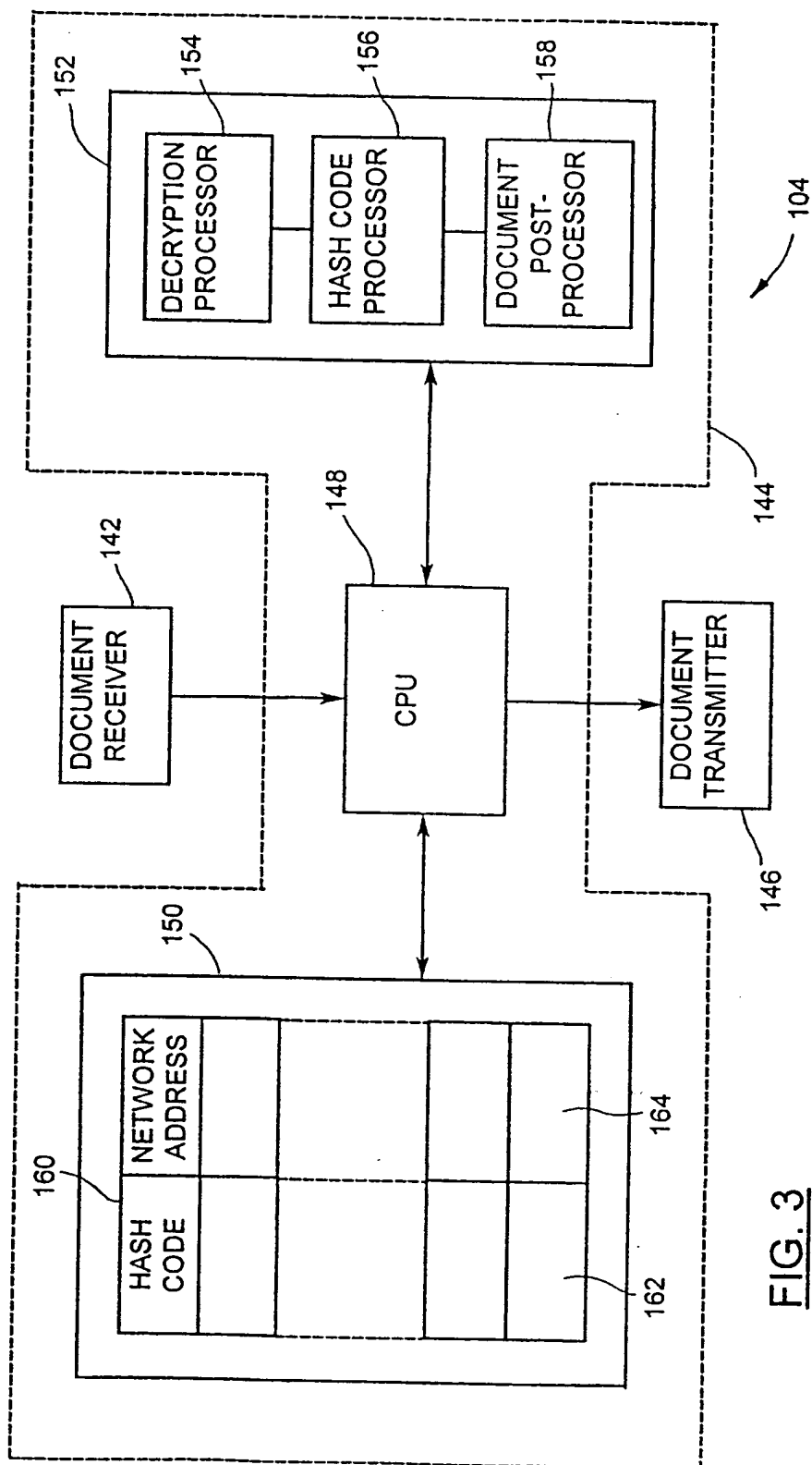


FIG. 3

4/6

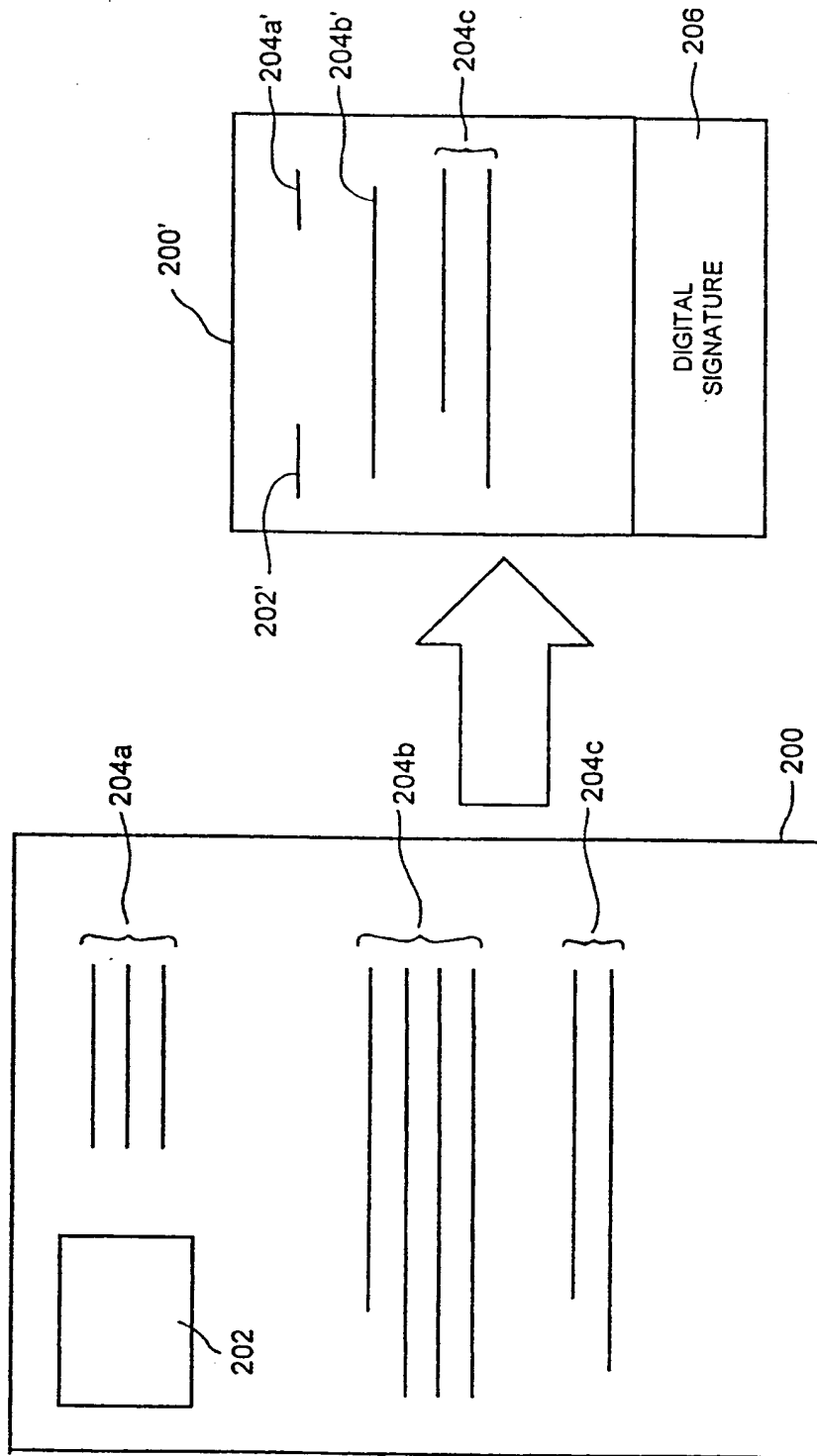


FIG. 4

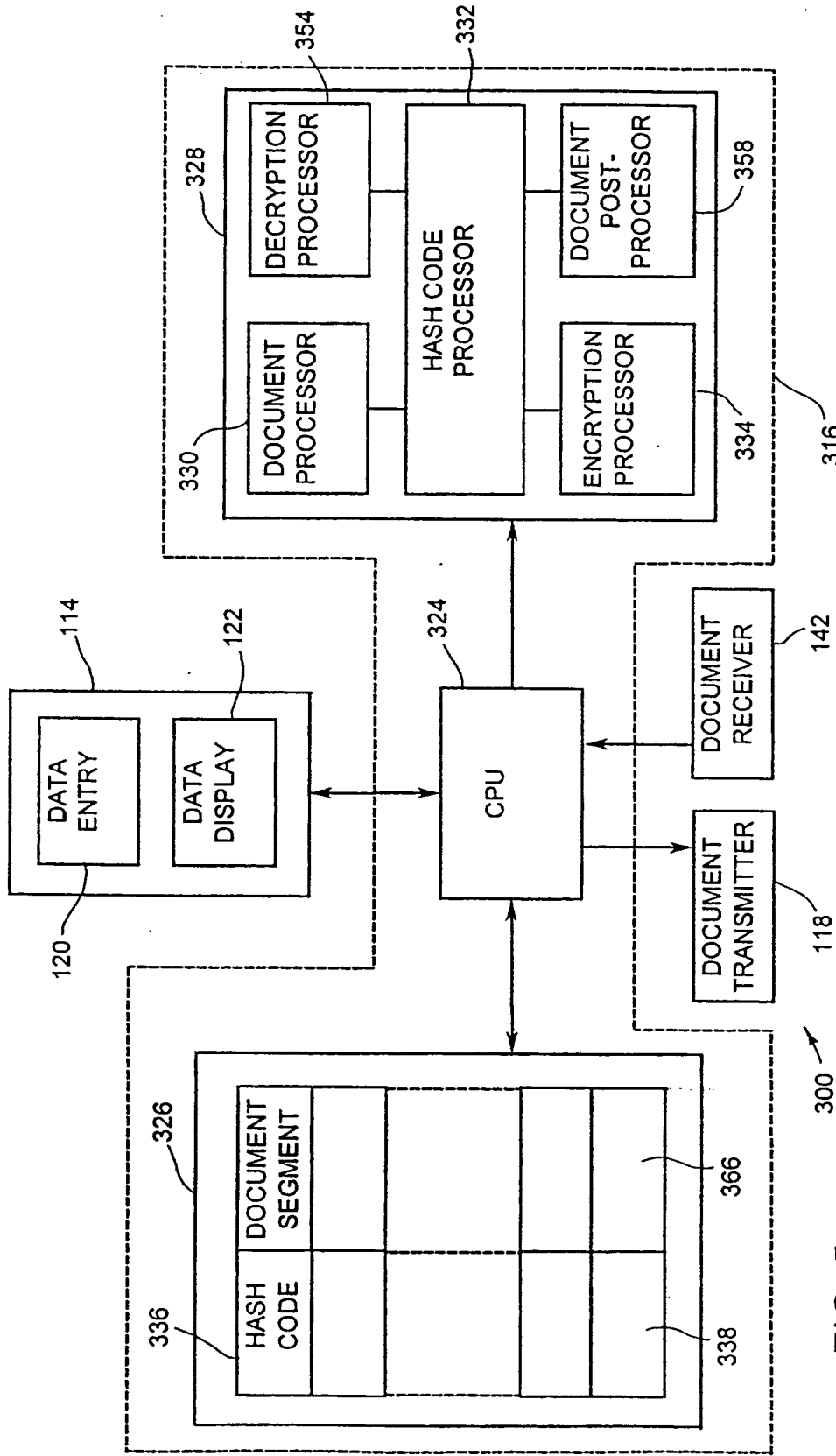


FIG. 5

6/6

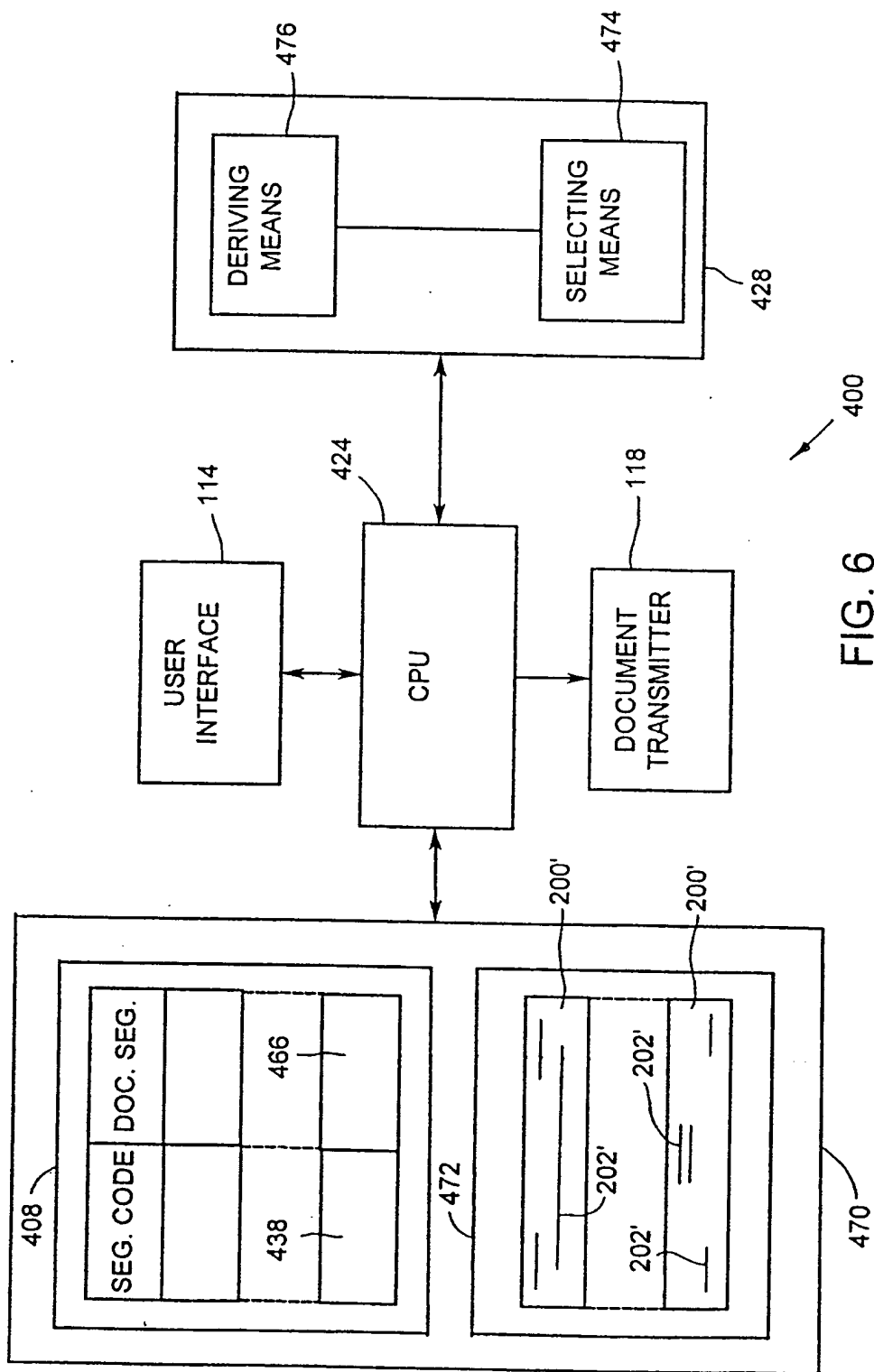


FIG. 6

INTERNATIONAL SEARCH REPORT

International Application No

PCT/CA 00/00292

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	WO 00 18060 A (POST OFFICE ;PERKINS RODNEY (GB)) 30 March 2000 (2000-03-30) abstract page 3, line 9 -page 4, line 4 page 4, line 17 -page 5, line 18	1, 12, 22, 29, 32, 33
A	EP 0 665 486 A (AT & T CORP) 2 August 1995 (1995-08-02) abstract column 1, line 34 -column 2, line 5 column 3, line 6 -column 4, line 32	1-33
A	US 5 487 100 A (KANE JOHN R) 23 January 1996 (1996-01-23) abstract column 1, line 65 -column 2, line 38 column 3, line 60 -column 4, line 9	1-33

☐ Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

30 August 2000

Date of mailing of the international search report

07/09/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Larcinese, C.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/CA 00/00292

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 0018060	A	30-03-2000	AU 6211199 A	10-04-2000
EP 0665486	A	02-08-1995	US 5509074 A	16-04-1996
			CA 2137065 A	28-07-1995
			JP 7239828 A	12-09-1995
US 5487100	A	23-01-1996	CA 2145874 A	14-04-1994
			CN 1088034 A,B	15-06-1994
			EP 0746936 A	11-12-1996
			WO 9408419 A	14-04-1994